
DB120-WL
4 Port Wireless ADSL2/2+ Modem
User Manual

V 1.0

CONTENTS

1. OVERVIEW.....	3
1.1 ABOUT ADSL.....	3
1.2 ABOUT ADSL2/2+	3
1.3 FEATURES	3
2 SPECIFICATION.....	4
2.1 INTERFACE INTRODUCTION.....	4
2.1.1 INDICATOR AND INTERFACE.....	4
2.1.2 SPLITTER SPEC	4
2.2 HARDWARE CONNECTION	4
2.3 LED STATUS INDICATION.....	5
3. CONFIGURATION.....	6
3.1 DEFAULT CONFIGURATION.....	6
3.2 COMPUTER CONFIGURATION	6
3.3 ADSL MODEM CONFIGURATION	6
3.3.1 LOG IN.....	6
3.3.2 SAVE SETTING.....	6
3.4 WAN CONFIGURATION	7
3.4.1 Vlew WAN Service	7
3.4.2 RFC1483 BRIDGE ON ATM CONFIGURATION	7
3.4.3 PPPOE ON ATM CONFIGURATION	9
3.4.4 IPOE ON ATM CONFIGURATION	12
3.5 WIRELESS CONFIGURATION.....	15
3.5.1 WIRELESS BASIC SETUP	16
3.5.2 WIRELESS SECURITY	16
3.5.3 WIRELESS MAC Filter.....	18
3.5.4 WIRELESS ADVANCED SETUp	19
4 OTHER CONFIGURATION	19
4.1 LAN CONFIGURATION	19
4.1.1 Configuration of Modem's password	19
4.1.2 CONFIGURATION OF MODEM'S IP ADDRESS.....	20
4.1.2 DHCP CONFIGURATION	21
5. TROUBLESHOOTING.....	21
5.1 UNABLE TO ACCESS INTERNET	21
5.1.1 CHECK THE LINE AND THE DEVICE	21
5.1.2 CHECK YOUR CONFIGURATION	22
ANNEX: SHIPPING LIST.....	23

1. OVERVIEW

1.1 ABOUT ADSL

An ADSL MODEM is a broadband Internet access device, which utilizes the high frequency segment of the phone line to transmit high-speed data without affecting the voice transmission. The frequency of the ADSL signal is higher than that of voice, so voice and ADSL signal can coexist in one line by using a splitter to insulate each from the other. ADSL data transfer adapts the asymmetry model. It supports upload transmission speed up to 1Mbps and download speed up to 8 Mbps (24Mbps for ADSL2+). ADSL is an ideal device for broadband access.

1.2 ABOUT ADSL2/2+

Transmission performance of ADSL2 is improved comparing with the first generation of ADSL. These improvements are mainly concerned with long distance, anti-line-loss, anti-noise, etc. By doubling the transmission bandwidth, ADSL2+ has implemented a downlink rate as high as 24 Mbps. Therefore, Internet applications such as synchronous transmission of multi video stream, online games and huge capacity of downloading files are made possible.

1.3 FEATURES

- 1、 Support ANSI T1.413 ISSUE 2, ITU G.992.1 (GDMT), ITU G.992.2 (GLITE), ITU G992.3, ITU G992.5
- 2、 Web-based configuration and monitoring.
- 3、 Support multiple PVCs.
- 4、 Routing function including static routing and RIP
- 5、 DNS function ,including DNS server , DNS Relay, DDNS
- 6、 NAPT, DHCP, Firewall, UPNP function.
- 7、 Quality of Service Control for Traffic Prioritization.
- 8、 Supports Virtual Private Network (VPN) pass-through.
- 9、 Support 802.11b, 802.11g.
- 10、 Support Multiple SSID
- 11、 Support Wireless MAC Filter, Wireless Bridge, and WPS (Push-Button and PIN).
- 12、 Diagnostics function.
- 13、 Support SNMP, TR069 and TR064 to manage the device.
- 14、 Access Control function.
- 15、 Device LOG function
- 16、 Update software via WEB, CLI, TR069

2 SPECIFICATION

2.1 INTERFACE INTRODUCTION

2.1.1 INDICATOR AND INTERFACE

Table 2.1

ITEM	Name	State introduction
Indicator	POWER	A steady Green light means the power connection works properly
	DSL	Green, show DSL line status.
	INTERNET	Green, Flashing means the Modem is transmitting or receiving data
	WLAN	Green, Indicates status of connection to the wireless device
Interface	LINE	Connected with phone line or “ADSL” port of the splitter.
	ETHERNET	To be connected to a PC network card by a straight-through network cable, also can use a crossover cable to connect to Hub, Switch or Router.
	POWER	Power interface, Connect with power adapter.
	SWITCH	To turn on / off the power.
	RESET	Press the reset button and turn on the power, then keep pressing the reset button for 3 seconds. Then you can reset the modem with the default settings.
	WIRELESS	Open/Close wireless via pressing the button

2.1.2 SPLITTER SPEC

Table 2.2

Interface	Introduction
LINE	Connected with telephone line
ADSL	Connect with the LINE port of the ADSL Modem using telephone line provided.
PHONE	Connect with telephone

2.2 HARDWARE CONNECTION

Introduction:

1. Use a telephone cord to connect the LINE port of the splitter with the RJ-11 port (the phone jack) on the wall.
2. Use another telephone cord to connect the ADSL port of the splitter with the LINE port of the ADSL Modem.
3. Use another telephone cord to connect the telephone set with the PHONE port of the splitter.
4. Connect Ethernet port of the ADSL MODEM with 10/100BASE-T port of the computer using the network cable that comes with the modem.
5. Plug in the power cord, and turn on the power.

If you do not want Internet services and telephone voice services simultaneously, please just connect the LINE port of the ADSL Modem with the RJ-11 port (the phone jack) on the wall using a telephone cord. In this case, the splitter is not necessary.

2.3 LED STATUS INDICATION

Table 2.3

Status	POWER (red)	DSL (green)	INTERNET (green)	WIRELESS(green)
Steady light	Power on	The modem is in good connection	/	Wireless is connected
Flashing	/	In handshaking status	/	/
Fast flashing	/	/	Transmitting or receiving data	Transforming data
Off	Power off	Connection not set up	Not connected with PC properly	Wireless is disabled

3. CONFIGURATION

3.1 DEFAULT CONFIGURATION

ADSL MODEM has pre-configured with the VCI/VPI which is in common use.

3.2 COMPUTER CONFIGURATION

The default IP address for ADSL MODEM is: **192.168.1.1**; The Subnet Mask is: **255.255.255.0**. Users can configure ADSL MODEM through an Internet browser. ADSL MODEM can be used as gateway and DNS server; users need to set the computer's TCP/IP protocol as follow:

- 1、 Set the computer IP address at same segment of ADSL MODEM, such as set the IP address of the network card to one of the “192.168.1.2”~ “192.168.1.254”.
- 2、 Set the computer's gateway the same IP address as the ADSL Modem's.
- 3、 Set computer's DNS server the same as ADSL Modem's IP address or that of an effective DNS server.

3.3 ADSL MODEM CONFIGURATION

3.3.1 LOG IN

Open the browser; input **http://192.168.1.1** at the address column. Press “Enter” key then the entry dialog box will show up as Figure 3.1. Input Username: admin, Password: admin (capital sensitive), then press Enter.

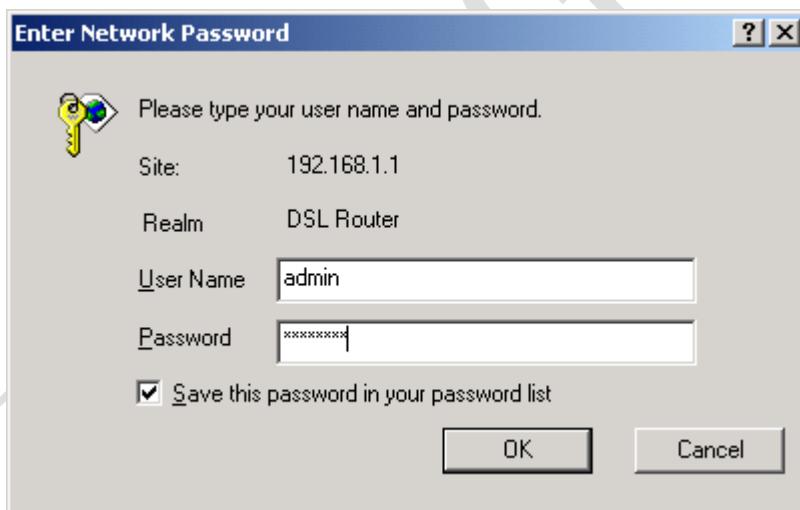


Figure 3.1

3.3.2 SAVE SETTING

After getting through each page for parameters setting, click “Save” or “Save/ Apply” to store the value in ADSL MODEM. Briefly, we named “Save”.

Note:

When you save the settings, the web page will be refreshed slowly, please wait it finished.
Some settings only take effect after rebooting the router.

3.4 WAN CONFIGURATION

If the configuration is bridge encapsulation, there is no need to configure any more parameters. Only need to use the third party dial-up software to connect the Internet.

Totally, this router supports: PPPoA, PPPoE, MER, IPoE, IPoA, Bridging. For detail configuration information, please check the following configuration guide.

3.4.1 VIEW WAN SERVICE

Click “Device Info” on the left page, and enter into “WAN” page.

- **NOTE: At most we can support eight connections. We support edit non-bridge wan connections. There is no need to reboot the device when you add/remove/edit one wan connection. It takes effect immediately.**

WAN Info									
Interface	Description	Type	VlanMuxId	IGMP	NAT	Firewall	Status	IPv4 Address	
atm0	br_0_0_35	Bridge	Disabled	Disabled	Disabled	Disabled	Unconfigured	0.0.0.0	
ppp0	pppoe_0_8_35	PPPoE	Disabled	Disabled	Enabled	Enabled	Unconfigured	(null)	

Figure 3.2

3.4.2 RFC1483 BRIDGE ON ATM CONFIGURATION

Click “Advanced Setup” on the left page, and enter into “Layer2 Interface” configuration page, where we can select the type of Layer2-Interface ATM.

- **NOTE: ATM interface is our most commonly used mode, which will transport data on DSL line via Bridge or Route Connections.**

Select ATM Interface, then click “Add” button to add one NEW Interface of Layer2. Then input Appropriate VPI/VCI, select EOA used for IPoE , PPPoE, Bridge, and select Encapsulation Mode and Service Category, Connection Mode (Default, VLAN-MUX, MSC). If QOS need, please select “Enable quality Service”. Usually, you only need to setup VPI/VCI to the value assigned by your ISP .At last click “Apply /Save” button to save the configuration.

Device Info
Quick Setup
Advanced Setup
Layer2 Interface
ATM Interface
WAN Service
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DSL
UPnP
DNS Proxy
Interface Grouping
LAN Ports
IPSec
Certificate
Multicast
Wireless
Diagnostics
Management

ATM PVC Configuration
This screen allows you to configure an ATM PVC Identifier (VPI and VCI), select DSL latency, select a service category5. Otherwise choose an existing Interface by selecting the checkbox to enable it.

VPI: [0-255]
VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
 EoA
 PPPoA
 IPoA

Select Connection Mode
 Default Mode - Single service over one connection
 VLAN MUX Mode - Multiple Vlan service over one connection
 MSC Mode - Multiple Service over one Connection

Encapsulation Mode:

Service Category:

Enabling IP QoS for a PVC improves performance for selected classes of applications. QoS can only be enabled for UBR without PCR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.
 Enable IP QoS

Figure 3.3

After your save, there will be one Layer2 Interface (atm2) added as following:

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	IP QoS	Scheduler Alg	Remove
atm0	0	35	Path0	UBR	EoA	DefaultMode	Disabled		<input type="checkbox"/>
atm1	8	35	Path0	UBR	EoA	DefaultMode	Disabled		<input type="checkbox"/>
atm2	8	81	Path0	UBR	EoA	DefaultMode	Disabled		<input type="checkbox"/>

Figure 3.4

Next, add one Layer3 Interface via “Wan Service” configuration page, and click “add” button as following:

Device Info
Quick Setup
Advanced Setup
Layer2 Interface
ATM Interface
WAN Service
Ethernet Mode
LAN
NAT
Security
Parental Control

Wide Area Network (WAN) Service Setup
Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	Edit
atm0	br_0_0_35	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>	<input type="button" value="Edit"/>
ppp0	pppoe_0_8_35	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

Figure 3.5

You need to select one Layer2 Interface from the Layer2Interface List. Then click “Next” to select Bridge mode:

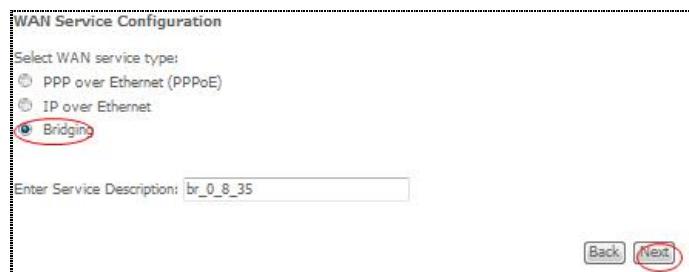


Figure 3.6

Press "Next" to enter into "WAN Setup - Summary", click "Apply/Save" to save configuration, if you need to modify the parameter, click "Back" as Figure 3.7.

WAN Setup - Summary

Make sure that the ~~the settings~~ below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

Figure 3.7

3.4.3 PPPOE ON ATM CONFIGURATION

PPPoE is also known as RFC 2516. It is a method of encapsulating PPP packets over Ethernet.

PPPoA is also known as RFC2364 and named as Peer to Peer Protocol over ATM. As PPPoE, it also has all the features of PPP. Although it's based on ATM protocol, the setting of all the other parameters is similar with PPPoE. So we only introduce PPPoE in detail here.

In Figure 3.6, select PPP over Ethernet (PPPoE)

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)

IP over Ethernet

Bridging

Enter Service Description:

[Back](#) [Next](#)

Figure 3.8

Press “Next” entering the configuring interface, as Figure3.9.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO

Enable Fullcone NAT

MAC Clones:

Dial on demand (with idle timeout timer)

Manual connect

PPP IP extension

NAT Public IP Address: Automatic Static Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

[Back](#) [Next](#)

Figure 3.9

- PPP Username: Your account from ISP to access Internet.
- PPP Password: Input the password assigned by your ISP.
- PPPoE Service Name: Server name of network ISP. No need to set.
- Authentication Method: Authentication mode of network ISP. Default is AUTO.
- Dial on demand: When this mode is selected, the connection that has no traffic within assigned disconnect

timeout (e.g. 1 minute) will be automatically disconnected. The connection will be activated again when traffic arrives. This function is advantageous for users who are charged with online time. It should be noticed that some programs automatically link to Internet. Computer will send data to network when infected by virus. Connection will not be disconnected under these data streams.

- Inactivity Timeout: When “Dial on demand” is selected, this input box indicates that after how long the connection will be disconnected in the absence of traffic. If the value is 0, connection will not be disconnected.
- Enable manual MTU set: set MTU value manually by yourself
- Manual Connect: connect/disconnect PPPoE connection manually

Press “Next” to select default gateway from Routing Interfaces:

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

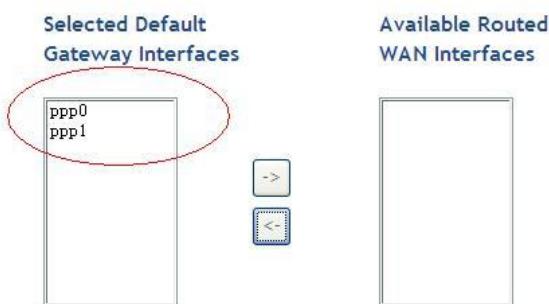


Figure 3.10

Press “Next” to setup default DNS server as following:

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces	Available WAN Interfaces
ppp0 ppp1	

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Figure 3.11

Press “Next” to enter into “WAN Setup - Summary”, click “Apply/Save” to save configuration, if you need to modify the parameter, click “Back” as Figure 3.12

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Figure 3.12

3.4.4 IPOE ON ATM CONFIGURATION

In Figure3.6, select MAC Encapsulation Routing (MER).

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description: ipoe_0_8_81

[Back](#) [Next](#)

Figure 3.13

Press “Next”, and the IP address can be queried from your ISP, the result as Figure3.14.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

- Obtain an IP address automatically
- Option 60 Vendor ID:
- Option 61 IAID: (8 hexadecimal digits)
- Option 61 DUID: (hexadecimal digit)
- Option 125: Disable Enable
- Use the following Static IP address:

WAN IP Address:	202.113.24.99
WAN Subnet Mask:	255.255.0.0
WAN gateway IP Address:	202.113.1.1

MAC Clone: [Clone the PC MAC Address](#)
 (00:00:00:00:00:00 means use dynamic mac address)

Figure 3.14

Press “Next” to configure services of Translation on this connection, as Figure 3.15:

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).



Figure 3.15

Press “Next” to select default gateway from Routing Interfaces as Figure 3.16:

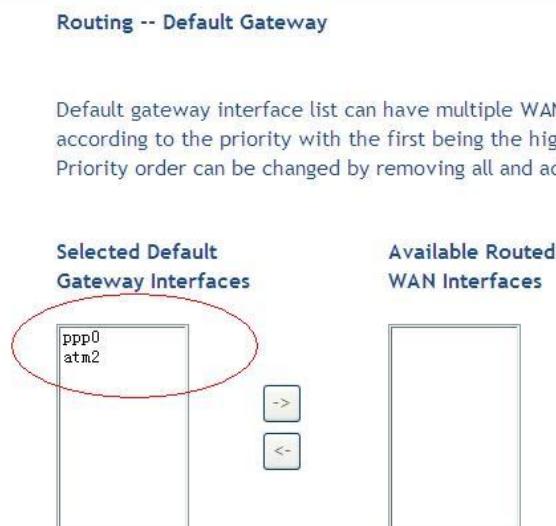


Figure 3.16

Press “Next” to setup default DNS server as Figure 3.17:

DNS Server Configuration

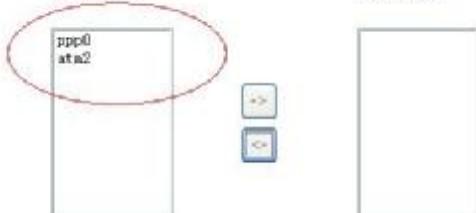
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, If only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN Interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

Available WAN Interfaces



Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Figure 3.17

Press “Next” to enter into “WAN Setup - Summary”, click “Apply/Save” to save configuration, if you need to modify the parameter, click “Back” as as Figure 3.18

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Figure 3.18

3.5 WIRELESS CONFIGURATION

Press “**Wireless**” on the top of web pages to enter wireless section. You can select to configure wireless setup, security and management.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

Click "Apply/Save" to configure the basic wireless options.

Enable Wireless

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Country:

Max Clients:

Figure 3.19

3.5.1 WIRELESS BASIC SETUP

Click “**Basic**” on the left menu to setup basic wireless parameters. In default, check “Enable Wireless” box to launch wireless AP.

- **SSID** (Service Set Identifier): The mobile users cannot access WLAN until setting their SSID as the same value of the wireless ADSL. The SSID value of the ADSL is “wireless”
- **Hide Access Point:** If checked, wireless station will no see SSID of the ADSL.

3.5.2 WIRELESS SECURITY

Press “**Security**” on the left menu to construct wireless security. You can select to configure WEP encryption, Shared, 802.1x, WPA, and WPA2 authentication.

- **WEP Encryption**
Select “Enabled” of the WEP encryption list. You can enter WEP encryption page.

Encryption Strength: Key length: 128bits or 64bits.

Network Key 1-4: Up to four keys that are in form of hex digits could be set. Mobile users can’t access the AP if they haven’t set the same key as AP. For 64bits and 128bits keys, you should input 10 and 26 hexadecimal digits or 5 and 13 ASCII characters respectively. Every two digits should be separated with others by a space character. For example: “7890ABCDEF” (hexadecimal digits) or “QWERT” (ASCII characters) for a key length of 64bits.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
 You may setup configuration manually
 OR
 through WiFi Protected Setup(WPS)

WSC Setup

Enable WSC

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	<input type="button" value="wireless"/>
Network Authentication:	<input type="button" value="Open"/>
WEP Encryption:	<input type="button" value="Enabled"/>
Encryption Strength:	<input type="button" value="128-bit"/>
Current Network Key:	<input type="button" value="1"/>
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys	
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys	

Figure 3.20

- 802.1x Authentication

Select “802.1x” to enter 802.1x authentication page.

The 802.1x authentication needs a Radius server in LAN. In this page, you can input Radius server IP address, port number and secret key.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	<input type="text" value="wireless"/>
Network Authentication:	<input type="text" value="802.1X"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
WEP Encryption:	<input type="text" value="Enabled"/>
Encryption Strength:	<input type="text" value="128-bit"/>
Current Network Key:	<input type="text" value="2"/>
Network Key 1:	<input type="text" value="1234567890123"/>
Network Key 2:	<input type="text" value="1234567890123"/>
Network Key 3:	<input type="text" value="1234567890123"/>
Network Key 4:	<input type="text" value="1234567890123"/>
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys	
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys	
<input type="button" value="Apply/Save"/>	

Figure 3.21

3.5.3 WIRELESS MAC FILTER

In fact, the Access List function is just like MAC address filtering and selected to permit or forbid access of wireless station with specified MAC address.

Method: select “Allow” or “Deny” mode, and click “Add” button, and input MAC address which you want to allow or deny.

<div style="border: 1px solid #ccc; padding: 5px;"> Device Info Quick Setup Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Diagnostics Management </div>	<p>Wireless -- MAC Filter</p> <p>MAC Restrict Mode: <input checked="" type="radio"/> Disabled <input type="radio"/> Allow <input type="radio"/> Deny</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 50%; text-align: center;"><input type="button" value="MAC Address"/></td> <td style="width: 50%; text-align: center;"><input type="button" value="Remove"/></td> </tr> <tr> <td style="text-align: center;"><input type="button" value="Add"/></td> <td style="text-align: center;"><input type="button" value="Remove"/></td> </tr> </table>	<input type="button" value="MAC Address"/>	<input type="button" value="Remove"/>	<input type="button" value="Add"/>	<input type="button" value="Remove"/>
<input type="button" value="MAC Address"/>	<input type="button" value="Remove"/>				
<input type="button" value="Add"/>	<input type="button" value="Remove"/>				

Figure 3.22

Notice: You only can select one of allow mode or deny mode.

3.5.4 WIRELESS ADVANCED SETUP

Press “Advanced” on the left menu to construct wireless security as Figure 3.23

Wireless – Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click “Apply/Save” to configure the advanced wireless options.

Band:	2.4GHz	Current: 11 (interference: acceptable)
Channel:	11	
Auto Channel Timer(min):	0	
54g™ Rate:	Auto	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
54g™ Mode:	802.11b Auto	
54g™ Protection:	Auto	
Preamble Type:	Long	
Transmit Power:	100%	

Figure 3.23

4 OTHER CONFIGURATION

4.1 LAN CONFIGURATION

4.1.1 CONFIGURATION OF MODEM’S PASSWORD

When you configure ADSL MODEM through an Internet browser, the system requires user name and password to validate access permission. The factory sets the modem at a default username of “**admin**” and the password of “**admin**”. The username is unchanged. You can enter the “password configuration” on Configuration column to change the password.

Attention: please remember the password after change, otherwise you will not be able to change configuration after saving setting as Figure 4.1

Device Info Quick Setup Advanced Setup Wireless Diagnostics Management Settings System Log SNMP Agent TR-069 Client Access Control Services Passwords IP Addresses Update Software Reboot Tools	Access Control -- Passwords <p>Access to your broadband router is controlled through three user accounts: admin, support, and user.</p> <p>The user name "admin" has unrestricted access to change and view configuration of your DSL Router.</p> <p>The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.</p> <p>The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.</p> <p>Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 15%;">Username:</td> <td><input type="text"/></td> </tr> <tr> <td>Old Password:</td> <td><input type="password"/></td> </tr> <tr> <td>New Password:</td> <td><input type="password"/></td> </tr> <tr> <td>Confirm Password:</td> <td><input type="password"/></td> </tr> </table> <p style="text-align: right;"><input type="button" value="Apply/Save"/></p>	Username:	<input type="text"/>	Old Password:	<input type="password"/>	New Password:	<input type="password"/>	Confirm Password:	<input type="password"/>
Username:	<input type="text"/>								
Old Password:	<input type="password"/>								
New Password:	<input type="password"/>								
Confirm Password:	<input type="password"/>								

Figure 4.1

4.1.2 CONFIGURATION OF MODEM'S IP ADDRESS

As a network device, ADSL Modem has its own IP address and MAC address. The factory sets the MODEM, at a default IP address of 192.168.1.1 and subnet mask of 255.255.255.0. The user can configure these addresses through the "LAN" on "Configuration" like this:

For example, change IP address to "10.10.10.10". Click "LAN", input "IP address": 10.10.10.10, then "subnet mask": 255.255.255.0, the result is as Figure 4.1, press "Apply/Save" as Figure 4.2.

Device Info Quick Setup Advanced Setup Layer2 Interface ATM Interface WAN Service Ethernet Mode LAN NAT Security Parental Control Quality of Service Routing DSL UPnP DNS Proxy Interface Grouping LAN Ports IPSec Certificate Multicast Wireless Diagnostics Management	<p>Local Area Network (LAN) Setup</p> <p>Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName <input type="button" value="Default"/></p> <table border="0" style="width: 100%;"> <tr> <td style="width: 15%;">IP Address:</td> <td><input type="text" value="192.168.1.1"/></td> </tr> <tr> <td>Subnet Mask:</td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td colspan="2"> <input type="checkbox"/> Enable IGMP Snooping <input type="checkbox"/> Enable LAN side firewall <input checked="" type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server Start IP Address: <input type="text" value="192.168.1.2"/> End IP Address: <input type="text" value="192.168.1.254"/> Leased Time (hour): <input type="text" value="24"/> </td> </tr> <tr> <td colspan="2"> <p>Static IP Lease List: (A maximum 32 entries can be configured)</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 15%;"><input type="button" value="MAC Address"/></td> <td style="width: 15%;"><input type="button" value="IP Address"/></td> <td style="width: 15%;"><input type="button" value="Remove"/></td> </tr> <tr> <td><input type="button" value="Add Entries"/></td> <td><input type="button" value="Remove Entries"/></td> <td></td> </tr> </table> </td> </tr> <tr> <td colspan="2"> <input type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN interface </td> </tr> </table>	IP Address:	<input type="text" value="192.168.1.1"/>	Subnet Mask:	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Enable IGMP Snooping <input type="checkbox"/> Enable LAN side firewall <input checked="" type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server Start IP Address: <input type="text" value="192.168.1.2"/> End IP Address: <input type="text" value="192.168.1.254"/> Leased Time (hour): <input type="text" value="24"/>		<p>Static IP Lease List: (A maximum 32 entries can be configured)</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 15%;"><input type="button" value="MAC Address"/></td> <td style="width: 15%;"><input type="button" value="IP Address"/></td> <td style="width: 15%;"><input type="button" value="Remove"/></td> </tr> <tr> <td><input type="button" value="Add Entries"/></td> <td><input type="button" value="Remove Entries"/></td> <td></td> </tr> </table>		<input type="button" value="MAC Address"/>	<input type="button" value="IP Address"/>	<input type="button" value="Remove"/>	<input type="button" value="Add Entries"/>	<input type="button" value="Remove Entries"/>		<input type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN interface	
IP Address:	<input type="text" value="192.168.1.1"/>																
Subnet Mask:	<input type="text" value="255.255.255.0"/>																
<input type="checkbox"/> Enable IGMP Snooping <input type="checkbox"/> Enable LAN side firewall <input checked="" type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server Start IP Address: <input type="text" value="192.168.1.2"/> End IP Address: <input type="text" value="192.168.1.254"/> Leased Time (hour): <input type="text" value="24"/>																	
<p>Static IP Lease List: (A maximum 32 entries can be configured)</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 15%;"><input type="button" value="MAC Address"/></td> <td style="width: 15%;"><input type="button" value="IP Address"/></td> <td style="width: 15%;"><input type="button" value="Remove"/></td> </tr> <tr> <td><input type="button" value="Add Entries"/></td> <td><input type="button" value="Remove Entries"/></td> <td></td> </tr> </table>		<input type="button" value="MAC Address"/>	<input type="button" value="IP Address"/>	<input type="button" value="Remove"/>	<input type="button" value="Add Entries"/>	<input type="button" value="Remove Entries"/>											
<input type="button" value="MAC Address"/>	<input type="button" value="IP Address"/>	<input type="button" value="Remove"/>															
<input type="button" value="Add Entries"/>	<input type="button" value="Remove Entries"/>																
<input type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN interface																	

Figure 4.2

4.1.2 DHCP CONFIGURATION

- click “LAN”
- click “DHCP server”;
- Define the “Start IP address” and the “End IP address” of DHCP server (for example, from 10.10.10.11 to 10.10.10.254).
- Input the value of lease (Measured by the second, 0 indicates permanently valid).

As Figure 4.3, open DHCP server, computer will set the IP Address of network card with one of the address 10.10.10.11 ~ 10.10.10.254.

○ Disable DHCP Server
 Enable DHCP Server
 Start IP Address: 10.10.10.100
 End IP Address: 10.10.10.200
 Leased Time (hour): 24
 Static IP Lease List: (A maximum 32 entries can be configured)
 MAC Address IP Address Remove
 Add Entries Remove Entries

Figure 4.3

Note: When you use the DHCP Server, please pay attention to having multi-DHCP Server in one LAN.

5. TROUBLESHOOTING

5.1 UNABLE TO ACCESS INTERNET

5.1.1 CHECK THE LINE AND THE DEVICE

- 1、Check the indicator of power supply is on, if not, Make sure the connection of power supply is correct; Make sure the output of power supply is correct; Make sure the switch of power supply is turned on;
- 2、Check the indicator of PC is on, if not, Make sure the connection of cable and network adapter; Make sure that the correct cable is used;
- 3、Check the LINK LED to see if it is twinkling. If no fast twinkling is observed within 3 minutes, please check whether phone line has been correctly placed; whether ADSL separator is correctly used. If multiple extensions have been installed, make sure that the separator is installed prior to the junction box of phone line. If the above items are confirmed and still no fast twinkling of WAN LED is observed, call the ISP to query whether ADSL service has been provided on your line;
- 4、Check the LINK LED to see whether it is unable to change status from fast twinkling to always light, or whether it changes status to fast twinkling after sometime of always light. If these phenomena occur constantly, please contact your ISP with a demand to check lines and signal quality;

If there is no problem in the above items, the line and the device shall be working. Problems may come

from your computer configuration or device configuration.

5.1.2 CHECK YOUR CONFIGURATION

We explain here the configuration of PPPOE using Windows 2000 operation system as an example. For other operation systems the process is similar.

- 1、 Enter the device manager to check if Ethernet adapter is correctly installed. If any problem exists, please re-installed it;
- 2、 Check the configuration of Ethernet adapter in PC. Try to manually set IP address that is in band 192.168.1.x without conflict. See 3.2;
- 3、 Try to run command “ping 192.168.1.1” on command line mode. If the response returns “time out”, please check Ethernet connection and IP settings;
- 4、 If this modem is reachable, try to run ping with a known outer IP, e.g. the DNS server IP of ShangHai Online: “ping 202.96.209.133”.
 - If ping is reachable, there shall be no problems in the modem. Please see step 5;
 - If ping is not reachable, see step 6 and check if the configuration is correct.
- 5、 Please try to ping a certain outer URL, e.g. “ping www.google.com”.
 - If ping is reachable, there shall be no problems in the network settings. Please check the settings of the PC terminal, e.g. whether the security level is too high, or whether anti-virus firewall is installed;
 - If ping is not reachable, check the DNS setting of Ethernet adapter. See 3.2.

Note 1: The precondition is that the LAN settings in the modem has not been modified.

Note 2: We usually start command line mode in Windows xp as follows: click on the “RUN” item of Windows Start Menu, input characters “cmd” in the input box popped up with an “Enter”. The window subsequently popped up is the command line window.

Note 3: The returned values of ping command in the following format show the standard of “reachable”

```

H:\WINNT\system32\cmd.exe

H:>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.1:
  Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

H:>

```

Figure 5.1

- 6、 If ping of the modem is reachable but ping of the outer fixed IP is unreachable, attention should be concentrated upon device settings. Please enter the configuring interface following the instructions in this manual.
 - (1) Check first the number of connections. If more than one connection exists, for troubleshooting , delete unused connections and remain the one connection you are using.

- (2) Check the connection to see whether correct “type” is selected. It’s normal to choose login type of PPPoE. When you use PPPoE to login, the following information should be provided: VPI and VCI, which can be queried from your ISP, user name and password.
- (3) Then make sure that “using NAT” and “default gateway” have been selected with a tick. Check whether “connect on demand” has been selected with a tick. If it is selected, the connection is activated only when traffic to outer networks arrives. If not selected, check “keep connection”, which should be set to 0 if you demand to keep connection

Make sure that the above parameters are saved after configuration. Internet is now available since the configuration is properly done.

ANNEX: SHIPPING LIST

ADSL MODEM	×1
User Manual	×1
Power Supply	×1
Cable Cat5 RJ45	×1
Telephone Line	×2
Warranty Certificate	×1

FCC Notice:

THIS DEVICE MUST NOT BE CO-LOCATED OR OPERATING IN CONJUNCTION WITH ANY OTHER ANTENNA OR TRANSMITTER

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Federal Communications Commission (FCC) Requirements, Part 15

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

REGULATORY INFORMATION / DISCLAIMERS

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the

equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

MPE Statement (Safety Information)

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

SAFETY INFORMATION

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.